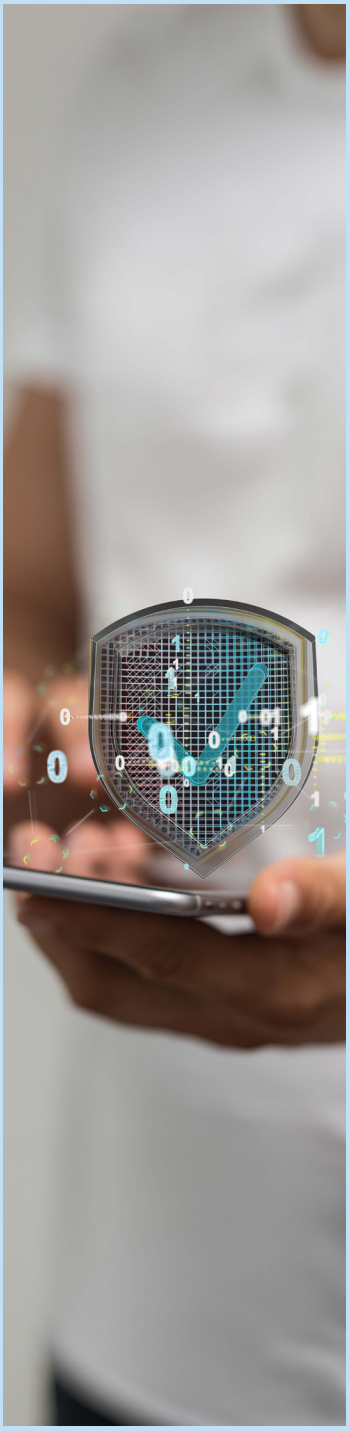
VIEW POINT



AI-DRIVEN FRAUD DETECTION: THE FUTURE OF DIGITAL TRUST

Abstract

AI-driven fraud detection is redefining how financial institutions protect digital trust in an era of fast-moving, sophisticated, and AI-enabled fraud. By shifting from static, rule-based controls to adaptive, context-aware intelligence, AI helps institutions detect anomalies in real time, reduce false positives, accelerate investigations, and respond more effectively to emerging fraud vectors such as deepfakes, synthetic identities, and real-time payment attacks. As digital transactions scale and threat actors become more agile, AI-led fraud detection is becoming a strategic capability for building resilience, improving customer experience, and sustaining trust across financial services.

Infosys®
Navigate your next

Whether it is a retail bank that holds the personal savings of citizens or a capital markets firm executing billion-dollar transactions across geographies, or even a payments network that is processing millions of micro-transactions by the day, every financial interaction is underwritten by a single assumption: that the parties involved are who they claim to be, and that the system works as promised. In essence, the financial services industry is a sector that is based on trust.

This trust is not incidental to the business of finance. It is the business. Regulatory frameworks, compliance structures, KYC protocols, and audit mechanisms all exist to protect and reinforce it. When trust is intact, capital flows freely, consumers transact confidently, and institutions operate efficiently. When trust erodes, the consequences cascade, from individual financial harm to systemic reputational damage.

This trust is not incidental to the business of finance: it is the business. All the products, platforms, and services of the industry are built around this fundamental tenet. All regulatory frameworks, compliance structures, Know Your Customer (KYC) protocols, fraud management solutions, and audit flows exist to protect and reinforce this tenet. For decades, financial institutions have built their fraud defences around rule-based systems such as pattern matching, threshold alerts, and manual review queues. However, these systems were fit for an earlier era that was defined by face-to-face transactions, paper trails, and a fraud landscape that moved at human speed.

That era is over.

Fraud: Evolving Faster Than Traditional Defences

What has changed is the operating environment. Financial institutions now operate in a vastly different marketplace where in-person transactions are getting rarer. Digital systems transacting billions of dollars in seconds rule the roost. Inter-country movement of money is common.

To add to all these, the threat landscape has undergone a structural shift. Fraud is no longer the work of isolated bad actors exploiting obvious vulnerabilities. It is an increasingly sophisticated and AI-augmented activity that operates at a scale that often overwhelms conventional detection systems. Such fraud can swiftly undermine the basic trust that is driving businesses and bring down great financial institutions.

Industry analysts point to five critical trends that financial institutions must urgently understand:

- The rise of AI-powered fraud tools available to criminals
- Deepfake-enabled identity fraud
- Synthetic identity creation at scale
- Real-time payment exploitation, and
- The blurring of cybercrime and financial fraud into unified attack vectors.

Each of these trends represents a qualitative shift in how fraud is designed and deployed.

In the meantime, the volume and velocity of digital financial transactions continue to grow exponentially. More transactions mean more surface area for fraud. More channels, such as mobile, embedded finance, and open banking APIs, mean more potential entry points. Traditional rule-based financial systems that are already straining under alert fatigue and high false-positive rates are being outpaced.

As of this writing, the market is rapidly consolidating around solutions that move beyond rules engines toward adaptive, intelligence-led detection. It is now a matter of speed: about how fast financial institutions can upgrade their fraud capabilities, and with which technology foundation.

AI: Giving Fraud Detection a Structural Advantage

Artificial intelligence does not merely improve fraud detection. It reframes the problem. Where

traditional systems ask, "Does this transaction match a known fraud pattern?" — AI systems ask, "Is this behaviour anomalous in context, and what is the probability that it signals risk?" This is not a subtle difference. It is the difference between a reactive posture and a predictive one.

For financial institutions, the deployment of Artificial Intelligence (AI)-driven systems can often provide the tipping point that takes them from a reactive posture to a predictive, proactive one.

There are three AI-driven capabilities that are fundamentally reshaping fraud detection in financial services:

Capability 1: Real-Time Behavioural Intelligence at Scale:

Modern AI-powered fraud detection systems process thousands of signals per transaction and evaluate them dynamically in milliseconds. These could include device fingerprints, behavioural biometrics, transaction velocity, geolocation, and network relationships. This is a capability that is not available with more traditional rules-based systems, which can only evaluate pre-defined conditions. Decision intelligence platforms combine Machine Learning (ML) with explainable AI to produce real-time risk scores that take into account the full complexity of a customer's behavioural context. For example, a spike in spending abroad may be preceded by the purchase of a plane ticket to travel to that country. Such analyses mean fewer false positives, more precise fraud catches, and friction applied only where it is genuinely warranted.

Capability 2: Agentic AI for Autonomous Fraud Investigation:

The deployment of Agentic AI to combat financial crime is a significant leap beyond traditional automation. Agentic AI systems do not merely flag suspicious activity: they go one step further and investigate it. Such systems can autonomously gather evidence across transaction histories, customer records, and external data sources; generate hypotheses about fraud typologies; and escalate only those cases that require human judgement.

The productivity implications of such autonomous systems operating at scale and with speed are substantial. Fraud investigation teams that were historically bottlenecked by alert volumes can now redirect their capacity toward complex, high-value cases that truly require human expertise. Routine fraud signals could be resolved without human touch. Analysts at McKinsey hail this as a transformation in how banks fight financial crime.

Capability 3: Adaptive Learning Against Emerging Fraud Vectors:

The most dangerous characteristic of modern fraud is its adaptability. Criminal networks are constantly probing financial systems for new vulnerabilities. They keep improving their techniques in response to newer detection methods. This highlights a key gap in traditional defenses: a fraud detection system that learns only from historical patterns will always be catching yesterday's attack.

AI systems trained on federated learning architectures and continuously updated on emerging fraud signals offer a structural counter to this dynamic. Adaptive analytics capabilities in AI systems now allow platforms to evolve alongside the threat landscape. When a new fraud typology emerges—whether it is a deepfake-enabled account takeover or a synthetic identity exploitation—adaptive AI systems can incorporate new signals and update their risk models in near-real time, without waiting for manual rule updates.

Ai-Driven Fraud Detection: The Future Of Digital Trust

AI-driven fraud detection is now a strategic imperative for financial institutions. Such systems offer enterprises an opportunity to build more resilient and competitive businesses that uphold the trust reposed in them by all stakeholders. The systems can help financial institutions combat fraud effectively, while continuing to pursue strategic growth goals in production innovation and improved customer outcomes

The threat landscape demands this shift. Institutions cannot risk falling behind in the war against adversaries who are actively accelerating their attack mechanisms. The analyst consensus is clear as well: Gartner's Magic Quadrant for Decision Intelligence Platforms and Forrester's Wave for Enterprise Fraud Management both reflect a market that has decisively shifted toward AI-led solutions. Market leaders in the fraud detection space offer systems that are distinguished by their machine learning depth, real-time decisioning capabilities, and explainable AI frameworks.

Digital trust has now emerged as a competitive advantage for financial institutions. Consumers and enterprise clients increasingly make financial relationships based on trust signals, not just rates and features. An institution that is known for seamless, low-friction experiences with strong fraud protection commands increased loyalty. Conversely, an institution that repeatedly fails to detect fraud, or one that creates excessive friction for legitimate customers through poorly calibrated controls, erodes the relationship. With its ability to personalise risk decisions, minimise false positives, and respond to threats in real time, AI-powered fraud detection is the capability layer that makes digital trust operationally real.

How Infosys BPM can Help

Fraud detection solutions from Infosys BPM employ AI algorithms for swift detection of fraudulent credit card transactions. Beyond detection, such solutions harness advanced analytics to derive actionable insights, bolstering fraud prevention efforts of enterprises. Talk to Infosys BPM to understand how AI-powered fraud detection solutions could power your industry and underwrite trust.

For more information, contact infosysbpm@infosys.com

Infosys®
Navigate your next